Information and Coding Theory (M. Tech. CrS)
Assignment 2021-2022

Those crediting the course should mail the complete answers in typed or legibly scanned work sheets in pdf format, mentioning their name and roll number, ***only to Questions (1-3) on or before Friday, 03.06.22****. Maximum score is* 15*, with* 5 *points in the wind.*

1. Design a binary code with length 10, minimum distance ≥ 6 and constant codeword weight 4 which achieves the relevant Johnson bound for size.

3 points

2. (a) Compute all the cyclotomic cosets defined by the powers of the primitive element $\alpha \in \mathbb{F}_{2^6}$, which is a root of $X^6 + X + 1$. Compute by hand the polynomials corresponding to the cyclotomic cosets defined by α^9 and α^{21}.
   Next compute, preferably using a program in C, Python or Sage, the respective polynomials corresponding to the remaining cyclotomic cosets. Include the program in your submission: full points only if it runs correctly!

   (b) Design BCH codes over $\mathbb{F}_{2^6}$, if possible, using combinations of the above cyclotomic cosets with:
   (i) code rate ~ 0.7, correcting at least 3 errors;
   (ii) code rate ~ 0.3, correcting at least 10 errors.
   Justify your answers.

8+4 = 12 points

3. Give a *complete* proof that a Goppa code can be obtained as the restriction of a suitable generalized Reed-Solomon (GRS) code to an appropriate subfield. (cf. Theorem 4, Chapter 12, MacWilliams and Sloane.)

5 points

Study Assignment: Not to be Submitted

4. The exercises in the study materials.
5. Binary Goppa codes: properties and examples (cf. Chapter 12, MacWilliams and Sloane's text).
6. Verify the steps of the instance of Berlekamp-Massey decoding for the triple error-correcting $(15, 9)$ Reed-Solomon code in Table 7.2, Chapter 7 of Blahut's text[1].
7. The evolution of ISD-based attacks in Bernstein *et al.*'s paper[2].
8. The NIST submission document for Classic McEliece: description of the protocols and discussion on achieving CCA security.

[1] R. E. Blahut, *Algebraic Codes for Data Transmission*, Cambridge Univ. Press, 2003

[2] Bernstein, Lange and Peters, "Attacking and defending the McEliece cryptosystem", PQCrypto 2008; LNCS-5299, Springer-Verlag.